

IN THE CLAIMS

Please cancel claims 2, 10, 11, 18, and 20.

Please amend the claims as follows:

---

1 1. (Amended) A communications system comprising:  
2 at least one communications server associated with at least one communications network;  
3 at least one communications terminal connected to the communications network to form  
4 a client-server relationship with the at least one communications server;  
A<sub>1</sub> 5 at least one policy definition point associated with said at least one communications  
6 server, said policy definition point defining policies for services, authentication, authorization,  
7 and accounting; and  
8 at least one policy enforcement point associated with said at least one communications  
9 terminal, wherein said policy enforcement point is operable to enforce on said communications  
10 terminal the policies defined in said policy definition point.

---

1 3.(Amended) The communications system according to claim 1, wherein said policy  
2 enforcement point includes means for enforcing policies pertaining to services, authentication,  
A<sub>2</sub><sup>3</sup> authorization and accounting.

1 4.(Amended) The communications system according to claim 1, wherein said policy  
2 enforcement point resides in said at least one communications terminal as a local policy

3 enforcement point.

1 5.(Amended) The communications system according to claim 1, wherein said at least one  
2 communications terminal is operable to support several simultaneously ongoing independent  
3 client-server relationships.

1 6.(Amended) The communications system according to claim 1, further comprising at least two  
2 mutually heterogeneous communication networks, wherein said at least one communications  
3 terminal is operable to exchange information with said at least two mutually heterogeneous  
communication networks.

A2  
Cov4

1 7.(Amended) The communications system according to claim 1, wherein said policy definition  
2 point is associated with at least one cluster of said at least one communications server.

1 8.(Amended) The communications system according to claim 7, wherein said policy definition  
2 point includes means for enacting policies in said at least one cluster of servers.

1 9.(Amended) The communications system according to claim 1, wherein said policy  
2 enforcement point includes means for enforcing a plurality of policies emanating from a plurality  
3 of networks and service providers.

---

1 12.(Amended) The communications system according to claim 1, wherein said policy definition  
2 point includes a global location register indicating in which of said at least one communications  
3 network said at least one communications terminal resides.

A3  
1 13.(Amended) The communications system according to claim 1, wherein said policy definition  
2 point further includes a subscriber database including means for storing subscriber IP addresses  
3 and encryption keys for each of a plurality of subscribers.

1 14.(Amended) The communications system according to claim 1, further comprising a credential  
2 verifier providing means for anonymous payment of access for at least one of said at least one  
3 communications network.

1 15.(Amended) The communications system according to claim 1, wherein said client-server  
2 relationship is provided by a transparent packet pipe transporting and classifying packets  
3 according to Quality of Service.

1 16.(Amended) A method for global roaming in a communications system, said method  
2 comprising the steps of:

3 forming a client-server relationship between at least one communications terminal and at  
4 least one communications server associated with at least one communications network;  
5 defining policies pertaining to services authentication, authorization, and accounting; and

6 enforcing the defined policies at a policy enforcement point associated with the  
communications terminal.

A3  
Incl.

1 17.(Amended) The method of claim 16, further comprising the step of defining policies in said  
2 policy definition point pertaining to services, authentication, authorization and accounting.

---

A4 1 19.(Amended) The method of claim 16, further comprising the step of defining, by said policy  
2 definition point, said policies in a plurality of server clusters.

---

A5 1 21.(Amended) The method of claim 16, further comprising the step of storing in said policy  
2 definition point subscriber IP addresses and encryption keys for each of a plurality of subscribers.

---

1 22.(Amended) The method of claim 16, further comprising the step of providing said  
2 client-server relationship by transporting and classifying packets according to Quality of Service.

1 23.(Amended) The method of claim 16, further comprising the step of providing separate  
2 charging mechanisms for access and services for client-server based transactions.

1 24.(Amended) The method of claim 16, further comprising the step of defining a policy domain  
2 having multiple policy blocks, each containing a specific relationship between a client and said at  
3 least one communications server.

25.(Amended) The method of claim 16, further comprising the steps of:

entering said policies in said policy enforcement point by a service provider; and  
updating said policies.

Please add the following new claims:

--26. (New) A method for anonymous payment of a subscriber for a service of a network, said

method comprising the steps of:

requesting a service by a subscriber using a mobile terminal;

transmitting encrypted payment information from the mobile terminal to an access node;

reading, by the access node, the encrypted payment information;

adding, by the access node, a transaction number to the encrypted payment information;

transmitting the encrypted payment information from the access node to a credential

verifier server identified in the payment information;

decrypting, by the credential verifier server, the encrypted payment information;

verifying, by the credential verifier server, whether the decrypted payment information is

correct;

transmitting the transaction number and a positive acknowledgment from the credential  
verifier server to the access node;

transmitting a message including an IP address and the positive acknowledgment from  
the access node to the mobile terminal; and

16 storing in a policy enforcement point the IP address associated with the service requested  
17 by the subscriber.

1 27. (New) The method of claim 26, further comprising the step of the policy enforcement point  
2 enabling the service requested by the subscriber.

1 28. (New) The method of claim 26, further comprising the steps of:

AL2 monitoring the transactions of the subscriber using the service; and

3 storing the transactions as accounting information.

1 29. (New) The method of claim 26, further comprising the step of ending the requested service  
2 by transmitting an end session message.

1 30. (New) The method of claim 26, further comprising the steps of:

2 sending the accounting information from the policy enforcement node to a secure mobile  
3 portal;

4 comparing the sent accounting information with accounting information generated in the  
5 secure mobile portal;

6 sending a positive accounting confirmation if the sent and generated accounting  
7 information correspond; and

8 sending a negative accounting confirmation if the sent and generated accounting

9 information do not correspond.

1 31. (New) A communications system comprising:

2 a policy definition point for defining policies for services, authentication, authorization,  
3 and accounting;

4 a policy enforcement point for enforcing the defined policies of a subscriber;

5 an access node for reading a credential verifier from a packet received from a mobile

Ab 6 terminal, adding a transaction number to the credential verifier, and forwarding the packet to the  
7 credential verifier specified in the packet;

8 a credential verifier for granting access to a particular service requested from the mobile  
9 terminal; and

10 a communications network for transporting data between said policy definition point, said  
11 policy enforcement point, said access node, and said credential verifier.

1 32. (New) the communications system of claim 31, wherein said policy enforcement point further  
2 comprises:

3 an authorization database for storing the policies defined in the policy definition point;

4 a policy enforcement point key for identifying the policy enforcement point to the policy  
5 definition point;

6 an authentication database for authenticating the subscriber and allowing access to the  
7 policy enforcement point; and

8 *AG*  
*concl.*

an accounting log for storing accounting information related to the service requested by

9 the subscriber.--

---